

**IN THE DRAWINGS**

The Examiner objected to Figures 2 and 3 of the drawings for not including the reference numbers 12 (PCF), 14 (PDSN), 20 (BSC), and 24 (MT). In response, Applicant has amended Figures 2 and 3 without adding new matter to indicate these reference numbers. Additionally, Applicant has amended Figure 2 to correct a minor typographical error not noted by the Examiner. Specifically, the labels "ALL REG. REQUEST" and "ALL REG. REPLY (ACCEPT)" have been amended to now reflect "A11 REG. REQUEST" and "A11 REG. REPLY (ACCEPT)." Applicant notes that the corrections to Figures 2 and 3 are shown in red, and requests that the Examiner hold the requirement for formal drawings in abeyance until a Notice of Allowance is issued.

### **REMARKS**

The present invention relates to an authentication method that provides replay protection at a packet control function (PCF). Specifically, the present invention guards against malicious replay attacks by performing verification checks on a 64-bit identification element contained in a registration reply message from a gateway, for example, a packet data service node (PDSN). The verification checks comprise comparing the entire 64-bits (i.e., a timestamp contained in the high-order 32 and the low-order 32 bits). If only the low-order 32 bits match, and a reply code in the reply message indicates an identification mismatch, the present invention compares the timestamp against a predetermined threshold. The reply message is valid provided the difference between the timestamp and the threshold falls within a valid range. The present invention further bolsters its protection by generating a sequential series of message numbers that are inserted into the low-order 32 bits of the identification element of successive registration request messages. In these embodiments, the registration reply message is valid if it contains both a valid timestamp and a valid message number. The timestamp in the identification element can then be used to synchronize the PCF clock with the PSDN clock.

### **35 U.S.C. §103 Rejections to claims 16, 36, and 41**

The Examiner rejected claim 16 under 35 U.S.C. §103(a) as being unpatentable over the "Request for Comments 2002" by Perkins (XP-002187650, hereinafter "RFC 2002") in view of Version 2 of the 3GPP2 Standard (XP-002233791, hereinafter "3GPP2 standard). Applicant respectfully disagrees. RFC 2002 discloses a method of replay protection. The 3GPP2 Standard teaches that RFC 2002 may be used for authentication of registration messages and registration reply messages transmitted between a PCF and PDSN. However, the combination of these references does not teach or suggest Applicant's claimed invention because RFC 2002 fails to teach or suggest using both a time stamp and message number to verify a registration

reply message as recited in the claims. As described in the application, RFC 2002 discloses two methods of protecting against a replay attack. The first method relies on a time stamp in the identification element. The second method relies on a nonce in the identification element. Using the time stamp method, the node sending the registration message (the PCF) inserts a 64-bit clock value into the identification element indicating the current time of day. The node receiving the registration message (the PDSN) verifies the time stamp and copies the low order 32-bits of the time stamp into the registration reply message. The PCF then verifies the registration reply message by comparing the low order 32-bits in the registration reply message to the low order 32-bits in the corresponding registration message sent by the PCF. There is no mention in RFC 2002 of using a message number to authenticate or verify the registration reply message.

As pointed out in the application, the time-stamp based method of replay protection is vulnerable to a replay attack because there is no assurance that the low order 32-bits of the time stamp are unique. Applicant's invention attempts to solve this problem by inserting a message number into the low order 32-bits of the identification element which is guaranteed to be unique within a predetermined time window. According to Applicant's invention, both the time stamp (high order 32-bits) and the message number (low order 32-bits) are used to verify the registration reply message. In RFC 2002, only the low order 32-bits of a time stamp are used for verification. RFC 2002 does not teach or suggest using a message number in combination with a time stamp to verify the registration reply message. Accordingly, the Examiner has failed to make a *prima facie* case of obviousness with respect to claims 16, 36, and 41.

**35 U.S.C. §103 Rejection to claim 30**

The Examiner also rejected claim 30 under 35 U.S.C. §103(a) as being unpatentable over Renaud (U.S. Patent Application Pub. No. 2001/0022823) in view of Parks (U.S. Patent Application Pub. No. 2001/0049285). Claim 30 is directed to a method of guarding against the erroneous re-synchronization of a reference time used by the PCF to time stamp its messages. According to claim 30, the PCF will adjust its reference time to a reference time received from the PDSN if a difference between the two does not exceed a pre-determined time threshold.

Renaud discloses a method of re-synchronizing a receiver's time clock to the time clock of a transmitter. According to Renaud, the receiver extracts a received timestamp. Renaud compares the timestamp to the receiver's internal clock to compute a time difference. Importantly, the receiver's clock is re-synchronized if the computed difference exceeds a predetermined threshold. *Renaud*, ¶ [0028]; Figs. 2, 3. Re-synchronization only if the difference exceeds a threshold is inapposite from re-synchronization if a computed difference does not exceed a threshold. Therefore, Renaud *teaches away* from claim 30, and the §103 rejection necessarily fails as a matter of law.

Further, Parks does not remedy this deficiency and the Examiner does not assert that it does. The Examiner merely cites Parks because it mentions 3G systems, and states that these systems inherently have PCFs and PDSNs. Regardless of what Park may or may not disclose, Renaud teaches away from claim 30.

Therefore, neither Renaud nor Parks teaches or suggests, alone or in combination, claim 30 or any of its dependent claims.

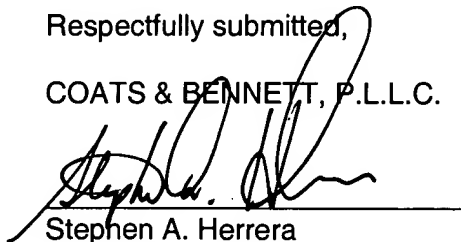
**Claim Amendments**

Finally, Applicant has amended claim 38 to correct the typographical error noted by the Examiner. Additionally, Applicant has also amended claim 16 to correct other typographical errors not noted by the Examiner, and to clarify claim 16. Specifically, claim 16 has been amended to clarify that the second registration message received at the PCF is responsive to the first registration message. Additionally, the message number in the second registration message is from the first registration message. None of the amendments add new matter.

In light of the foregoing remarks, Applicant respectfully requests allowance of all pending claims.

Respectfully submitted,

COATS & BENNETT, P.L.L.C.



Stephen A. Herrera  
Registration No.: 47,642

Dated: January 17, 2006

P.O. Box 5  
Raleigh, NC 27602  
Telephone: (919) 854-1844  
Facsimile: (919) 854-2084